**Amendments to the CLAIMS**

This listing of claims will replace all prior versions and listings of claims in the application.

**Listing of the CLAIMS**

1. (currently amended) A method of processing data, encrypted according to an encryption method specific to a first domain such that the~~y~~ data cannot be decrypted without the aid of a first secret specific to said first domain, said data being received in a presentation device connected to a network belonging to a second domain, wherein ~~it~~ the method comprises the steps ~~consisting, for the presentation device, in~~ of:

(a) transmitting to a processing device connected to the network at least a portion of said encrypted data ;

(b) receiving processed data from said processing device, at least one element being used to decrypt said received data with the aid of a second secret specific to said second domain, said second secret being contained in the presentation device.

2. (currently amended) The method as claimed in claim 1, wherein:

the data received in the presentation device are encrypted with the aid of a first symmetric key, said first symmetric key being received with said data in a form encrypted with the aid of the first secret;

~~in that~~ step (a) ~~consists in~~ comprises transmitting to the processing device the first symmetric key encrypted with the aid of the first secret; and

~~in that~~ step (b) ~~consists in~~ comprises receiving from the processing device:

- said first symmetric key encrypted with the aid of a second symmetric key; and

- the second symmetric key encrypted with the aid of the second secret ~~($K_{N2}$)~~ specific to the second domain.

3. (currently amended) The method as claimed in claim 2, wherein it also comprises the steps ~~consisting, for the presentation device, in~~ of:

(c) decrypting, with the aid of the second secret, the second encrypted symmetric key;

(d) decrypting, with the aid of the second symmetric key, the first encrypted symmetric key; and

(e) decrypting the data received by said presentation device with the aid of the first symmetric key.

4. (currently amended) The method as claimed in claim 3, ~~wherein it also comprises~~ comprising, before step (a), ~~a step consisting, for the presentation device, in~~ generating a random number,

said random number being transmitted to the processing device, in step (a), with the encryption of the first symmetric key;

and in that the data received in step (b) contain a random number and the first symmetric key encrypted with the aid of the second symmetric key;

step (d) also comprising the decryption, with the aid of the second symmetric key, of the encrypted random number received in step (b); and

the method also comprising, before step (e), a verification step to verify that the random number decrypted in step (d) is identical to the random number generated before step (a)~~; step (e) being performed only in the event of positive verification~~.

5. (currently amended) The method as claimed in claim 1, wherein a domain identifier is contained in the data received by the presentation device and

in that said domain identifier is transmitted to the processing device during step (a)~~;~~

~~step (b) being performed only if said processing device contains the same domain identifier~~.